BACKBEND (Malware Family)

By Fraunhofer FKIE

FireEye describes BACKBEND as a secondary downloader used as a backup mechanism in the case the primary backdoor is removed. When executed, BACKBEND checks for the presence of the mutexes MicrosoftZj or MicrosoftZjBak (both associated with BACKSPACE variants). If either of the mutexes exist, the malware exits.

▶ [TLP:WHITE] win_backbend_auto (20251219 | Detects win.backbend.)
